

**PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA
INFORMACIÓN**

TERMINAL DE TRANSPORTES DE MANIZALES S.A

SI-1600-1-1-009

DEPENDENCIA DE SISTEMAS

DIRIGIDO A:

GERENCIA

ENERO 30 DE 2024

**PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y
PRIVACIDAD DE LA INFORMACIÓN**

PRESENTÓ

ADRIANA LUCIA NARANJO PINEDA
Profesional Universitaria
Dependencia de Sistemas

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CONTENIDO

1.	INTRODUCCIÓN	3
2.	OBJETIVOS	4
	OBJETIVO GENERAL	4
	OBJETIVOS ESPECÍFICOS	4
3.	CONTEXTO ESTRATÉGICO.....	4
4.	ALCANCE.....	5
5.	POLÍTICA DE ADMINISTRACIÓN DEL RIESGO.....	5
6.	TÉRMINOS Y DEFINICIONES.	6
7.	MARCO NORMATIVO	9
8.	DESARROLLO DEL PLAN DE TRATAMIENTO DE RIESGOS Y PRIVACIDAD DE LA INFORMACION	10
9.	CLASIFICACIÓN DE LOS RIESGOS SOBRE LOS ACTIVOS DE TECNOLOGIA DE INFORMACIÓN.	11
10.	CRONOGRAMA PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	13
11.	INDICADOR	13
12.	VIGENCIA	13

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1. INTRODUCCIÓN

La gestión del **plan de tratamiento de riesgos de seguridad y privacidad de la información** son aquellos procesos que reducen las pérdidas y brindan protección de la información, permitiendo conocer las debilidades que afectan durante todo el ciclo de vida del servicio. Todos los servidores públicos en cumplimiento de sus funciones están sometidos a riesgos que pueden hacer fracasar una gestión; por lo tanto, es necesario tomar las medidas, para identificar las causas y consecuencias de la materialización de dichos riesgos.

Cualquier tipo de organización independiente de su tamaño y tipo afronta factores tanto internos como externos que pueden afectar uno de los activos más importante de la entidad que es la información. Todas las actividades de una entidad involucran riesgos y de una forma u otra los gestionan mediante su identificación, análisis y su respectivo tratamiento.

Por esa razón, el presente plan tiene como objetivo orientar y facilitar la implementación y desarrollo de una eficaz, eficiente y efectiva gestión del riesgo, desde la identificación hasta el monitoreo; enfatiza en la importancia de la administración del riesgo, sus fundamentos teóricos y de una orientación para facilitar su identificación, reconocimiento de las causas, efectos, definición de controles y de lineamientos sencillos y claros para su adecuada gestión.

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2. OBJETIVOS

OBJETIVO GENERAL

Definir las actividades, lineamientos y factores determinantes que permitirán llevar a cabo la gestión para el tratamiento de los riesgos de seguridad de la información, identificados en la Terminal de Transportes de Manizales S.A.

OBJETIVOS ESPECÍFICOS

- Definir las actividades requeridas para la implementar al tratamiento de riesgos de seguridad de la información.
- Evaluar el nivel de riesgo actual con el impacto generado después de implementar el plan de tratamiento de riesgos de seguridad de la información.
- Realizar seguimiento y control a la eficacia del plan de tratamiento de riesgos de seguridad de la información.

3. CONTEXTO ESTRATÉGICO

El presente plan está alineado y contribuye al logro de la misión, visión y demás elementos del direccionamiento estratégico de la Terminal de Transportes de Manizales S.A., los cuales se estipulan en el Plan Estratégico Institucional.

ARTICULACIÓN CON EL CONTEXTO ESTRATÉGICO	
APORTES AL DIRECCIONAMIENTO ESTRATÉGICO	<ul style="list-style-type: none"> ✓ Fortalecer los Sistemas Información ✓ Fortalecer el uso de las tecnologías de la información ✓ Optimizar los procesos misionales ✓ Mejorar los procesos administrativos
GESTIÓN Y DESEMPEÑO INSTITUCIONAL	<ul style="list-style-type: none"> ✓ Política de Gobierno Digital ✓ Política de Seguridad Digital

“Ser el punto de conexión con lo que más quieres”

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

	<p>✓ Política de transparencia, acceso a la información pública y lucha contra la corrupción</p>
--	---

La gestión de los riesgos de seguridad de la información son aquellos procesos que reducen las pérdidas y brindan protección de la información, permitiendo conocer las debilidades que afectan durante todo el ciclo de vida del servicio.

Se define el **Plan de Tratamiento de Riesgos de seguridad y privacidad de la información** como el proceso mediante el cual se identifica, comprende, evalúa, y mitiga cualquier tipo de riesgo o amenaza en la información de una determinada organización. Dentro de dicho plan, se contempla la identificación de activos informáticos, las vulnerabilidades y amenazas a los que se encuentran expuestos, así como su probabilidad de ocurrencia y el impacto de estas; lo anterior con el fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.

4. ALCANCE

El **Plan de Tratamiento de Riesgos de seguridad y privacidad de la información** es de estricta aplicabilidad y cumplimiento por parte de todos los servidores públicos y contratistas que presten sus servicios o tengan algún tipo de relación con la Entidad; dicho tratamiento de riesgo debe involucrar a todos los procesos y actividades desarrolladas por la Terminal de Transportes de Manizales S.A., en especial aquellos que impactan directamente la consecución de los objetivos misionales.

5. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

Según Resolución GE-1000-8-2-0003 de febrero 10 de 2022, se actualizo la Política de Administración del Riesgo, el cual tiene como **Objetivo** : Establecer parámetros para administrar los riesgos de la Terminal de Transportes de Manizales S.A., con el fin de aplicar medidas necesarias que permitan crear una base confiable para la toma de decisiones, asignar y utilizar eficazmente los recursos para el tratamiento de los riesgos y asegurar de esta forma el logro de los objetivos institucionales y de los procesos, y la cual hace parte integral del Plan de tratamiento de riesgos de seguridad y privacidad de la información.

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

6. TÉRMINOS Y DEFINICIONES.

Activo: En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

Administración de Riesgo: Actividad encaminada a la intervención de los riesgos de la entidad, a través de la identificación, valoración, evaluación, manejo y monitoreo de estos de forma que se apoye el cumplimiento de los objetivos de la entidad.

Análisis de Riesgo: Determinación del impacto en función de la consecuencia o efecto y de la probabilidad de ocurrencia del riesgo.

Apetito de riesgo: Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

Capacidad de riesgo: Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.

Causas: Medios, circunstancias, situaciones o agentes generadores del evento.

Causa Inmediata: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

Causa Raíz: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.

Consecuencia: Hechos o acontecimientos que se derivan o resultan de la ocurrencia o la materialización de un riesgo.

Control: Acciones encaminadas a educir la probabilidad de ocurrencia o el impacto que pueda generar la materialización de un riesgo.

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad.

Evento: Hecho que se genera durante la gestión de un proceso afectando el logro del objetivo del mismo, tiene relación directa con las actividades críticas de los planes operativos, las actividades de ruta crítica de los proyectos de inversión y las actividades críticas de control de los procesos.

Factores de Riesgo: Son las fuentes generadoras de riesgos.

Frecuencia: Periodicidad con que ha ocurrido un evento.

Gestor del Riesgo: funcionario líder de la dependencia, quien apoya al responsable del riesgo.

Identificación del Riesgo: Descripción de la situación no deseada.

Impacto: Magnitud de las consecuencias que puede ocasionar a la entidad la materialización del riesgo.

Integridad: Propiedad de exactitud y completitud.

Mapa de riesgos: Herramienta metodológica que permite hacer un inventario de los riesgos por proceso, haciendo la descripción de cada uno de ellos, las posibles consecuencias y su forma de tratamiento.

Nivel de riesgo: Es el valor que se determina a partir de combinar la probabilidad de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo poder ser Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, ejemplo, mediante una matriz de Probabilidad - Impacto.

Plan Anticorrupción y de Atención al Ciudadano: Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.

Políticas de Administración del Riesgo: Son los Criterios que orientan la toma de decisiones para tratar, y en lo posible minimizar los riesgos de la entidad, en función de su evaluación.

Probabilidad: Medida para estimar la posibilidad de que ocurra un evento.

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Responsable del Riesgo: Es el encargado de identificar, valorar y definir el plan de contingencia, el manejo y monitoreo para cada uno de los riesgos del proceso bajo su responsabilidad.

Riesgo: Posibilidad de ocurrencia del evento que tiene un efecto positivo o negativo sobre el producto o servicio generado de un proceso o el cumplimiento de los objetivos institucionales.

Riesgo Residual: Es aquel que continúa aún después de aplicar controles para mitigar el riesgo.

Riesgo Inherente: Es el riesgo puro, al cual no se han aplicado controles, para controlar y buscar evitar su materialización.

Riesgo de Seguridad de la Información: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

Riesgo de Corrupción: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

Tratamiento: Opciones que determinan el tipo de acciones a implementar para administrar el riesgo.

Tratamiento del riesgo: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad.

Valoración: Grado de exposición al riesgo con la clasificación de probabilidad e impacto aplicando los controles existentes.

Vulnerabilidad: Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

7. MARCO NORMATIVO

Ley 44 de 1993: "Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944." (Derechos de autor).

Ley 527 de 1999: "Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones".

Ley 1273 de 2009: "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

Ley 1581 de 2012: "Por la cual se dictan disposiciones generales para la protección de datos personales".

Decreto 19 de 2012: "Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública".

Decreto 1377 de 2013: "Por el cual se reglamenta parcialmente la Ley 1581 de 2012, Derogado Parcialmente por el Decreto 1081 de 2015".

Ley 1712 de 2014: "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones".

Decreto 1081 de 2015: "Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República."

Decreto 1078 de 2015: Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

Decreto 1499 de 2017, el cual modificó el Decreto 1083 de 2015 – Modelo Integrado de Planeación y Gestión.

Decreto 1008 de 2018: Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

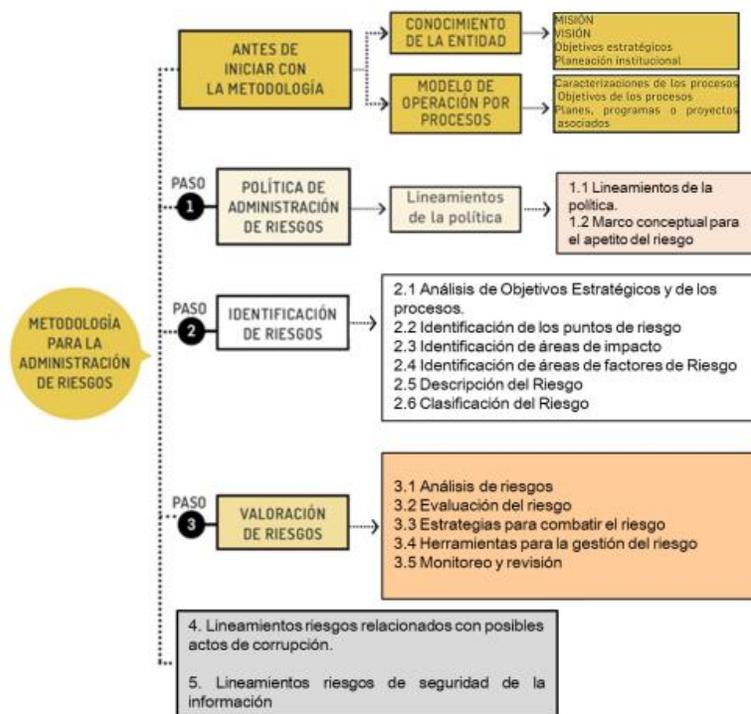
PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Guía para la administración del riesgo y el diseño de controles en entidades públicas, del Departamento Administrativo de la Función Pública.

8. DESARROLLO DEL PLAN DE TRATAMIENTO DE RIESGOS Y PRIVACIDAD DE LA INFORMACION

El desarrollo el **Plan de Tratamiento de Riesgos de seguridad y privacidad de la información**, tiene como propósito es la identificación, estimación y evaluación de los riesgos de **la Terminal de Transportes de Manizales S.A.**, para definir un plan de tratamiento que se ajuste a los objetivos de cada uno de los procesos. La Gestión de Riesgos de **la Terminal de Transportes de Manizales S.A.**, incluyendo los Riesgos de Seguridad y Privacidad se lleva a cabo por los Líderes de cada proceso y lo gestionan para el cumplimiento de la misión, visión y objetivos misionales, con el fin de determinar el tratamiento del riesgo aceptable sobre cada uno de los riesgos identificados, teniendo en cuenta el siguiente esquema:

Metodología para la administración de riesgo



Fuente: Elaborado y actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

“Ser el punto de conexión con lo que más quieres”

Carrera 43 No. 65-100 Los Cambulos Teléfonos 87 85641 – 87 87 858 – 87 87 832

Email – gerencia@terminaldemanzales.com.co

www.terminaldemanzales.com.co

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Beneficios de la administración en la Gestión de Riesgos

Considerando que la gestión del riesgo es un proceso efectuado por la alta dirección de la entidad y por todo el personal con el propósito de proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos, los principales beneficios para la entidad son los siguientes:

- Apoyo a la toma de decisiones
- Garantizar la operación normal de la organización
- Minimizar la probabilidad e impacto de los riesgos
- Mejoramiento en la calidad de procesos y sus servidores
- Fortalecimiento de la cultura de control de la organización
- Incrementa la capacidad de la entidad para alcanzar sus objetivos
- Dota a la entidad de herramientas y controles para hacer una administración más eficaz y eficiente

La Terminal de Transportes de Manizales S.A., sigue los lineamientos trazados por el Gobierno Nacional en cumplimiento de la Ley de Transparencia y acceso a la información y en la Política de Gobierno Digital, buscando fortalecer la relación Ciudadano - Estado, mejorando la prestación de servicios por parte de las entidades, y generando confianza en las instituciones que conforman la administración pública y el Estado en general, a través del uso y aprovechamiento de las TIC, las cuales se integran al Modelo Integrado de Planeación y Gestión - MIPG y a las políticas de Gestión y Desempeño Institucional.

9. CLASIFICACIÓN DE LOS RIESGOS SOBRE LOS ACTIVOS DE TECNOLOGIA DE INFORMACIÓN.

Todas las organizaciones deben implementar planes para gestionar los riesgos que afectan a los sistemas de información, tecnologías de información y activos informáticos, considerando que en la actualidad los riesgos más comunes son generados por ataques dirigidos al software empresarial, afectando la disponibilidad e integridad de la información almacenada o transportada a través de los equipos de comunicación.

Por esta razón hay que estar preparados para prevenir todo tipo de ataques o desastres, ya que cuando el costo de recuperación supera al costo de prevención es preferible tener implementados planes de gestión de riesgos que permitan la continuidad de la operación tras sufrir alguna pérdida o daño en la información de la entidad.

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Es por ello que **La Terminal de Transportes de Manizales S.A.**, identifico los riesgos de acuerdo a la Guía para la administración del riesgo del Departamento Administrativo de la Función Pública.

REFERENCIA	NOMBRE DEL RIESGO	CALIFICACION		ZONA DE RIESGO INHERENTE	TRATAMIENTO DEL RIESGO
		PROBABILIDAD INHERENTE (1-5)	IMPACTO INHERENTE(1-5)		
R1	Pérdida, fuga y/o borrado de datos de los servidores o unidades de almacenamiento	5	3	ZONA RIESGO ALTA	Reducir
R2	Ataques informáticos a los aplicativos y página web institucional	5	4	ZONA RIESGO ALTA	Mitigar
R3	Sistema de información susceptibles de manipulación o adulteración	5	3	ZONA RIESGO ALTA	Reducir
				ZONA RIESGO EXTREMA	
				ZONA RIESGO ALTA	
				ZONA RIESGO MODERADA	
				ZONA RIESGO BAJA	

Una vez definidos y valorados los riesgos a los que se encuentra expuesta la entidad, se efectúa un análisis de los controles preventivos o correctivos con los que cuenta la Dependencia de Sistemas.

No. DEL RIESGO	NOMBRE DEL RIESGO	DESCRIPCIÓN (Control al riesgo)	RESPONSABLE	VALORACIÓN DE CONTROLES										CALIFICACIÓN DEL ESTADO	CALIFICACIÓN DEL CONTROL	CONTROL DEL RIESGO			
				RESPONSABLE		ATRIBUTOS						EVIDENCIA DE LA EJECUCIÓN DEL CONTROL							
				ASESIGNACIÓN DEL RESPONSABLE	SEGREGACIÓN Y AUTORIDAD DEL RESPONSABLE	PERIODICIDAD	PROPÓSITO	CÓMO SE REALIZA LA ACTIVIDAD DE CONTROL	QUE PASA CON LAS OBSERVACIONES O DESVIACIONES	EVIDENCIA DE LA EJECUCIÓN DEL CONTROL									
R1	Pérdida, fuga y/o borrado de datos de los servidores o unidades de almacenamiento	Copias de seguridad de las bases de datos y de las unidades de almacenamiento	Sistemas	ASIGNADO	ADECUADO	OPORTUNA	PREVENIR	CONFIABLE	SE INVESTIGAN Y RESUELVEN OPORTUNAMENTE	COMPLETA	15	15	15	15	15	15	10	100	Fuerte
R2	Ataques informáticos a los aplicativos y página web institucional	Uso de Antivirus y Seguridad Perimetral, Plan de Seguridad y Privacidad de la Información.	Sistemas	ASIGNADO	ADECUADO	OPORTUNA	PREVENIR	CONFIABLE	SE INVESTIGAN Y RESUELVEN OPORTUNAMENTE	COMPLETA	15	15	15	15	15	15	10	100	Fuerte
R3	Sistema de información susceptibles de manipulación o adulteración	Plan de Seguridad y Privacidad de la Información, Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y definición de controles de acceso	Sistemas	ASIGNADO	ADECUADO	OPORTUNA	PREVENIR	CONFIABLE	SE INVESTIGAN Y RESUELVEN OPORTUNAMENTE	COMPLETA	15	15	15	15	15	15	10	100	Fuerte

Tras el análisis de los controles existentes, se plantearán las acciones de respuesta ante la materialización de los riesgos que se encuentren en categoría extrema, alta y moderada.

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

10. CRONOGRAMA PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

A continuación, cronograma propuesto para el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información en la Terminal de Transportes de Manizales S.A.

 TERMINAL DE TRANSPORTES DE MANIZALES S.A.														
CRONOGRAMA PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN														
ACTIVIDADES	VIGENCIA 2024													PRODUCTO / EVIDENCIA
	Meta	Fecha de Reporte o Ejecución de la actividad												
		Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic	
Actualizar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia 204	100%	X												
Renovar Licenciamiento del Antivirus	100%							X						
Realizar las copias de respaldos de información de la infraestructura de TI de la Terminal (Equipos y servidores)	100%	X	X	X	X	X	X	X	X	X	X	X	X	X
Realizar monitoreo de control de software instalado y gestión de capacidad de licenciamiento.	100%						X							
Levantar la Matriz Razi	100%			X										
Levantar Plan de continuidad de los servicios	100%			X										

11. INDICADOR

Número de actividades del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información desarrolladas / Número total de actividades del plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información programadas *100.
Periodicidad. Semestral.

12. VIGENCIA

El Presente Plan de Seguridad y Privacidad de la Información, entra en vigor a partir de su adopción y publicación.

Manizales, enero 30 de 2024